The Biggest Cybersecurity Risk Isn’t Technology-It’s Complacency

ARTICLE 09.01.26 THOUGHT LEADERSHIP

Why organizations that treat cybersecurity as an IT issue are falling behind-and what business leaders should do instead.

Cybersecurity has never been solely about technology. It is about risk, resilience, and leadership.

Yet many organizations continue to approach cybersecurity as an IT responsibility rather than an enterprise-wide business imperative. That mindset may be the greatest cybersecurity risk organizations face today.

While companies invest in new security tools, cybercriminals are evolving even faster. Artificial intelligence is enabling more convincing phishing and impersonation attacks, ransomware groups are operating like sophisticated businesses, and supply-chain compromises continue to expose organizations of every size. The technology available to defend against these threats has never been better-but technology alone cannot compensate for complacency.

Recent headlines reinforce the point. Financial institutions have faced sophisticated voice-phishing campaigns aimed at stealing credentials, while attackers continue to exploit trusted software, vendors, identities, and human behavior. Phishing-including voice and SMS-based variants-remains the costliest way in, averaging $5.29 million per incident in 2026. No organization is immune. The question is not whether your organization could become a target. It is whether you are prepared when it does.

Cybercriminals Are Running Businesses-and They Are Getting Better at It

The image of a lone hacker working from a basement is long outdated. Today’s cybercriminals operate like sophisticated enterprises. They use subscription-based ransomware services, recruit affiliates, buy stolen credentials, maintain specialized teams, and rapidly change names and infrastructure to evade law enforcement and security defenses.

Artificial intelligence is accelerating this evolution. Attackers can use AI to create persuasive phishing messages, imitate trusted voices, automate reconnaissance, write or modify malicious code, and scale social-engineering

campaigns that once required substantial time and expertise.

The result is not simply more attacks. It is a threat environment in which attacks can become faster, more personalized, and more difficult for employees and conventional controls to recognize.

The Cost of Complacency Is Rising

Organizations can no longer assume that prior investments, a clean audit, or the absence of a major incident means their security program is effective. Cyber risk changes as organizations adopt new systems, migrate to the cloud, acquirecompanies, add vendors, deploy AI tools, and expand remote access.

IBM’s 2026 Cost of a Data Breach Report found that the average global cost of a breach rose to $4.99 million. A 12% increase and a new record high driven attacks were a major driver, surging 56% year over year to account for more than one in four malicious breaches-and among organizations that experienced an AI-related breach, 92% lacked proper AI access controls. Those findings illustrate a broader lesson-rapid AI adoption without corresponding security governance creates security debt.

The financial impact is only part of the story. A cyber incident can disrupt operations, delay customer service, trigger legal and regulatory obligations, increase insurance costs, damage trust, and consume leadership attention for months.

Why Mid-Market Organizations Are Attractive Targets

Many executives still believe their organization is not large or prominent enough to attract cybercriminals. In reality, mid-market organizations often possess the same valuable assets as larger enterprises, including:

- Financial and payroll data
- Customer, patient, employee, or member information
- Intellectual property and proprietary business information
- Access to larger customers, vendors, and supply chains
- Operational systems that cannot tolerate extended downtime

At the same time, these organizations may have smaller security teams, aging systems, competing technology priorities, and limited visibility across their environments. Attackers understand this imbalance. They do not need to target the largest organization if they can profitably compromise several less-prepared ones-or use a smaller organization as an entry point into a larger ecosystem.

In an interconnected economy, your cybersecurity posture is no longer only your concern. Customers, business partners, insurers, regulators, lenders, and boards increasingly expect organizations to demonstrate that controls are not merely documented, but operating effectively.

Technology Alone Will Not Solve the Problem

Firewalls, endpoint detection and response, multi-factor authentication, email filtering, cloud security platforms, backups, and monitoring tools are all essential. But cybersecurity is not a product an organization can buy once and consider complete.

Many successful attacks do not defeat security technology head-on. Instead, attackers exploit compromised identities, misconfigurations, delayed patching, weak vendor oversight, excessive access, untested response plans, or employees who have not been prepared for increasingly convincing social engineering.

Cybersecurity is a capability an organization must build and continuously improve. Effective programs align people, processes, governance, and technology with the risks that matter most to the business.

Cyber Resilience Is a Business Imperative

The goal is not to eliminate every cyber risk. That is neither practical nor possible. The goal is to make informed decisions, reduce the likelihood and impact of incidents, detect threats earlier, and recover operations more confidently.

Boards and executive teams should be able to answer questions such as:

- What are our most significant cyber risks, and how have they changed?
- Which critical systems and business processes would create the greatest disruption if unavailable?
- How quickly could we detect, contain, and recover from a ransomware or identity-based attack?
- Have we tested our incident response and business continuity plans under realistic conditions?
- Which third parties create the greatest concentration of risk?
- Are our security investments aligned with our actual risk-or are we simply adding more tools?

These are not technical questions. They are business questions, and they require clear, business-focused answers.

How Dean Dorton Helps Organizations Move from Concern to Confidence

Dean Dorton helps organizations address cybersecurity, IT audit, and compliance as connected business disciplines rather than isolated projects. Two offerings sit at the center of that work: Fractional CISO leadership that gives organizations experienced security leadership on an ongoing basis, and AI security governance that helps organizations adopt AI safely as usage-and AI-driven attacks-continue to accelerate. Our integrated approach is

designed to help leadership understand current exposure, prioritize investments, verify that controls work, and build a more resilient security program.

Depending on an organization's needs and maturity, our team can assist with:

- Fractional CISO (vCISO) and information security leadership-embedded, ongoing executive guidance to build, mature, and govern a cybersecurity program without the cost of a full-time hire
- AI security governance and risk assessments to help organizations deploy AI tools safely, scope access to models and data, and close the AI governance gaps attackers are actively exploiting
- Cybersecurity assessments that identify risk, test key controls, and establish a practical improvement roadmap
- Managed detection and response to improve visibility, investigation, and response to potential threats
- Incident response, forensic support, tabletop exercises, and recovery planning
- Technical security testing, including vulnerability, penetration, red-team, and purple-team activities
- Third-party risk assessments, security awareness, and organizational risk assurance
- SOC reporting, outsourced or co-sourced IT audit, and IT general controls testing
- Regulatory compliance readiness and testing for requirements such as CMMC, DFARS, HIPAA, GLBA, PCI, SOX, ISO 27001, FDIC expectations, and applicable privacy laws
- Cybersecurity framework evaluations using recognized standards such as NIST, CIS, COBIT, ISO 27001, and related frameworks
- IT risk assessments and policies and procedures development or review

The right starting point will differ by organization. Some need an independent assessment of their current posture. Others need ongoing leadership, stronger detection capabilities, regulatory readiness, or a tested response plan. The objective is not to apply a generic checklist. It is to create a clear, risk-based path that supports the organization's operations and strategic goals.

Five Questions Every Board and Executive Team Should Ask

1

What are our top three cyber risks today-and who owns them?

2

If ransomware disrupted operations tomorrow, how quickly could we recover?

3

How do we know that our critical security controls are actually working?

4

Which vendors or business partners create our greatest cyber exposure?

5

Are we treating cybersecurity as an enterprise risk-or merely as an IT expense?

If leadership cannot answer these questions with confidence, that is not a reason for alarm-it is a reason to establish a clearer view of risk and a practical plan for improvement.

The Best Time to Strengthen Cybersecurity Is Before You Need It

Organizations rarely emerge from a major incident believing they prepared too much. More often, they wish they had identifiedweaknesses sooner, clarified responsibilities, tested recovery plans, improved visibility, or challenged assumptions about controls that appeared adequate on paper.

Complacency can take many forms: assuming that cyber insurance will absorb the impact, believing a managed service provider owns all security risk, relying on a compliance report as proof of resilience, or postponing improvements because no serious incident has occurred yet.

The threat landscape will continue to evolve. Artificial intelligence will make some attacks faster and more convincing. Regulatory and contractual expectations will continue to rise. Customers and business partners will demand greater assurance.

Organizations that treat cybersecurity as a strategic business capability-not simply an IT function-will be better positioned to protect operations, preserve stakeholder trust, and respond decisively when adversity strikes.

At Dean Dorton, we help organizations move beyond reacting to cyber threats. We help them build the governance, controls, detection capabilities, and resilience needed to navigate an increasingly complex digital environment.

A practical next step

An independent cybersecurity assessment, a Fractional CISO engagement, or an AI security governance review can help leadership understand where the organization stands, identify the most important gaps, and prioritize a roadmap based on business risk.

Talk to Our Security Team

Selected Sources and Further Reading

- Financial Times, “Big US Hedge Funds Targeted by Wave of Cyber Attacks,” August 6, 2026. Read more
- IBM, “Cost of a Data Breach Report 2026: The AI Tipping Point,” 2026. Read more
- Dean Dorton, “Cybersecurity, IT Audit, & Compliance.” Learn more
- Dean Dorton, “Comprehensive Cybersecurity Services for Your Business.” Learn more